Deutscher Bundestag **Drucksache 18/13271**

18. Wahlperiode 31.07.2017

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan van Aken, Annette Groth, Inge Höger, Ulla Jelpke, Alexander Ulrich, Kathrin Vogler und der Fraktion DIE LINKE.

Cyberübungen der EU und der NATO und ihr mögliches Überschreiten der Schwelle eines bewaffneten Angriffs

Am 7. September 2017 will der informelle EU-Verteidigungsministerrat in Tallinn (Estland) die Cyberübung „EU CYBRID 2017“ abhalten (http://gleft.de/1NL). Damit will die Europäische Union die gemeinsame strategische Krisenreaktion auf einen großen Cyberangriff proben (http://gleft.de/1NM). Die Übung steht unter der Verantwortung des Europäischen Auswärtigen Dienstes und soll das Bewusstsein für „Cybereffekte“ auf politischer und ministerieller Ebene schärfen. Zu probende Szenarien sind bislang nicht bekannt. Die Fragesteller gehen aber davon aus, dass es um die Kooperation der zuständigen operationellen Hauptquartiere in den EU-Mitgliedstaaten geht. Ebenfalls unklar ist, ob sich die Cyberübung auch oberhalb der Schwelle eines bewaffneten Angriffs bewegt. Dies würde bedeuten, dass der Cyberraum zum Austragungsort eines Konfliktes wird, der durch einen konventionellen Angriff auf einen Mitgliedstaat begann.

Für die Vorbereitung der Cyberübung hat die estnische Regierung jetzt eine Ausschreibung veröffentlicht (http://gleft.de/1NN). „EU CYBRID 2017“ findet unter estnischer Präsidentschaft statt. Womöglich aus diesem Grund wird die Übung möglicherweise gemeinsam mit dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) organisiert, das sich ebenfalls Tallinn befindet. Erste Gespräche des estnischen Verteidigungsministeriums mit der NATO hierzu haben bereits stattgefunden. Ebenfalls im September will die Europäische Union die fünfwöchige „Krisenmanagementübung 2017 – EU PACE17“ starten (http://gleft.de/1Og). Sie verfolgt sie ähnliche Ziele und Szenarien wie „EU CYBRID 2017“ und findet in einem Setting regelmäßiger Cyberangriffe sowie zunehmender „Fake News“ mit fünf „Bedrohungen“ statt. Hierzu gehören die Bekämpfung von „Migrantenschmuggel“; die Politik gegenüber einem Staat der wirtschaftlich und militärisch mächtiger wird, aber der westlichen Welt zuwiderlaufende Interessen vertritt und hierzu gut ausgebildete Hacker sowie staatliche Medien in Stellung bringt; eine terroristische religiöse Sekte, die ein weltweites Kalifat errichten will; eine globalisierungskritische Gruppe die gut in Sozialen Medien vertreten ist und militante Proteste organisiert und hierzu finanzielle Mittel von Ländern erhält, die der Europäischen Union feindlich gegenüberstehen; sowie zwei Akteure im Cyberraum mit dem Kürzel „APT“, die militärische Einrichtungen und Ölkonzerne als Hacker angreifen und dabei mit dem Staat in Verbindung stehen, der der westlichen Welt zuwiderlaufende Interessen vertritt.

Mit „Locked Shields“ hält die NATO selbst Cyberübungen ab. Zuletzt wurde die jährliche Übung vom 24. bis zum 28. April in Tallinn durchgeführt (http://gleft.de/1NP). Beteiligt waren mehrere europäische Verteidigungsministerien sowie das Europa-Kommando der USA. In Schlussfolgerungen fordert der Rat der

EU eine engere Zusammenarbeit der NATO und der Europäischen Union gegen Cyberangriffe und „hybride Bedrohungen“ (http://gleft.de/1NO). Zur Kooperationen gehören außerdem Trainingskurse und Cyberübungen. Zur Abwehr „hybrider Bedrohungen“ haben die Europäische Union und die NATO außerdem ein „Zentrum gegen hybride Bedrohungen“ („Hybrid-Kompetenzzentrum“) in Helsinki eingerichtet.

Wir fragen die Bundesregierung:

1. Was ist der Bundesregierung über die Teilnehmenden und Durchführenden der Cyberübung „EU CYBRID 2017“ sowie etwaiger Vorübungen bekannt, und wann genau finden diese statt?
2. Was ist der Bundesregierung über die Teilnehmenden und Durchführenden der Krisenmanagementübung „EU PACE17“ sowie etwaiger Vorübungen bekannt, und wann genau finden diese statt?
3. Mit welchen Abteilungen nehmen die Verteidigungsministerien der EU- und NATO-Mitgliedstaaten an den beiden Übungen teil, und welche Teile der Übungen finden gemeinsam statt?
4. Welche „Bedrohungen“ werden für die beiden Übungen angenommen und inwiefern trifft es zu, dass diese in einer Umgebung regelmäßiger Cyberangriffe sowie zunehmender „Fake News“ stattfinden?
5. Welche Szenarien werden (auch in Kombination) in „EU CYBRID 2017“ und „EU PACE17“ bzw. etwaigen Vorübungen durchgespielt (bitte so detailliert wie möglich schildern)?
   a) Inwiefern sollen sich die Übungen bzw. etwaige Vorübungen auch mit einem Eingreifen oberhalb der Schwelle eines bewaffneten Angriffs befassen, und welche Haltung vertritt die Bundesregierung hierzu?
   b) Welche Reaktionen (auch im Cyberraum) sollen auf einen solchen Angriff durchgespielt werden (bitte möglichst die simulierten Angriffe und Gegenangriffe schildern)?
   c) Sofern die Bundesregierung zu den Szenarien noch keine Informationen erhalten hat, wann sollen diese vorliegen?
6. Wann sollen welche „Injektionen” (etwa zur Eskalation der geübten „Krisen“ und „Bedrohungen“) im Rahmen von „EU CYBRID 2017“ und „EU PACE17“ erfolgen?
7. Inwiefern sollen auch die Verteidigungsminister selbst an „EU CYBRID 2017“ oder „EU PACE17“ beteiligt werden, und nach welchem Verfahren sollen diese auf die Szenarien reagieren?
8. Welche Aufgaben werden das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), die „EU Hybrid Fusion Cell” sowie das Kommunikationszentrum „EU STRATCOM EAST“ im Rahmen der Übungen übernehmen?
9. Welche „Injektionen” (etwa zur Eskalation der geübten „Krisen“ und „Bedrohungen“) wird die NATO im Rahmen der Übungen „EU CYBRID 2017” und „EU PACE17” vornehmen, und inwiefern stehen diese im Kontext der NATO-Übung „NATO CMX 17“?
10. Wann beginnt und endet die Übung „NATO CMX 17“, und wer nimmt daran teil?
11. Welche Szenarien hat das NATO-CCDCoE nach Kenntnis der Bundesregierung auf der jüngsten Cyberübung „Locked Shields“ durchgespielt (bitte möglichst die simulierten Angriffe und Gegenangriffe schildern)?

Vorabfassung - wird durch die lektorierte Version ersetzt.

12. Welche weiteren Cyberübungen sind auf Ebene der NATO und der Europäischen Union nach Kenntnis der Bundesregierung in Planung?

13. Welche weiteren Anstrengungen unternehmen die Europäische Union und die NATO nach Kenntnis der Bundesregierung 2017 hinsichtlich gemeinsamer Trainings oder der Durchführung von Cyberoperationen?

14. Was ist der Bundesregierung über den Stand der Einrichtung eines „Zentrums gegen hybride Bedrohungen“ („Hybrid-Kompetenzzentrum“) in Helsinki bekannt, wer arbeitet dort mit, und welche Aufgaben werden dort übernommen?

15. Inwieweit liegen der Bundesregierung mittlerweile neuere belastbare Erkenntnisse zur Urheberschaft des Angriffswerkzeugs „Stuxnet“ vor, den sie als „Cyber-Sabotage auf Kritische Infrastrukturen“ bezeichnet, und mit welchem Ergebnis sind die vorliegenden Erkenntnisse durch das Bundesamt für Verfassungsschutz „hinsichtlich einer möglichen nachrichtendienstlichen Urheberschaft bewertet worden“ (Bundestagsdrucksache 18/164, Frage 42)?

16. Was ist der Bundesregierung über Planungen der US-Übung „Cyber Storm 2018“ des Heimatschutzministeriums bekannt, und inwiefern erwägt sie wieder eine Teilnahme (Bundestagsdrucksache 18/4286)?

17. An welchen Übungen oder Trainings hat das Bundeswehrkommando „Computer-Netzwerk-Operationen“ (CNO) seit seiner Gründung teilgenommen (Bundestagsdrucksache 18/4286, Frage 1)?

18. Inwiefern hat das CNO in der Vergangenheit auch geübt, „in gegnerische Netzwerke einzudringen, dort aufzuklären, einzelne Funktionen zu stören und zeitweise außer Betrieb zu setzen oder dauerhaft zu schädigen“ (Bundestagsdrucksache 18/4286, Frage 13)?

19. Wie oft ist das deutsche „Netzwerk gegen hybride Bedrohungen“ seit Beantwortung der Bundestagsdrucksache 18/11543 (Frage 22) bereits zusammengekommen, und welche Themen standen dabei auf der Tagesordnung?

    a) Welche einzelnen Arbeiten werden im Netzwerk von den Bundesministerien, dem Bundeskanzleramt, der Beauftragten der Bundesregierung für Kultur und Medien sowie dem Bundespresseamt übernommen?

    b) Inwiefern wurden im Netzwerk auch Leitungs-oder Sekretariatsaufgaben vergeben, und von wem werden diese übernommen?

20. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat, bzw. liegen ihr hierzu nach wie vor keine Informationen darüber vor, dass es eine derartige, nicht von Staaten ausgeübte versuchte oder erfolgreich ausgeführte Attacke jemals gegeben hat (Bundestagsdrucksachen 17/7578, 18/164, 18/10759)?

Berlin, den 31. Juli 2017

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333